CLAIM AMENDMENTS

Listing of Claims:

CLAIMS

1. (currently amended) A method for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network, the method comprising: identifying data traffic on the network originating at any assigned address and addressed to any unassigned address, said unassigned address is an address which is free and not assigned to user systems; inspecting any data traffic so identified for data indicative of an attack; and, on detection of data indicative of an attack, generating an alert signal.

2. (original) A method as claimed in claim 1, wherein the inspecting comprises spoofing replies to requests contained in the data traffic identified.

3. (original) A method as claimed in claim 1, comprising, on generation of the alert signal, rerouting any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to a disinfection address on the network.

4. (original) A method as claimed in claim 1, comprising, on generation of the alert signal, sending an alert message to the disinfection address.

5. (original) A method as claimed in claim 5, wherein the alert message comprises data indicative of the attack detected.

6. (original) A method as claimed in claim 5, comprising, on receipt of the alert message, sending a warning message from the disinfection address to the address assigned to the data processing system originating the data indicative of the attack.

7. (original) A method as claimed in claim 6, comprising including in the warning message program code for eliminating the attack when executed by the data processing system originating the data indicative of the attack.

8. (currently amended) Apparatus for detecting attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network, the apparatus comprising: an intrusion detection sensor for identifying data traffic on the network originating at any assigned address and addressed to any unassigned address, said unassigned address is an address which is free and not assigned to user systems inspecting any data traffic so identified for data indicative of an attack, and, on detection of data indicative of an attack, generating an alert signal.

9. (original) Apparatus as claimed in claim 8, wherein the intrusion detection sensor in use inspects the data traffic identified by spoofing replies to requests contained in the data traffic identified.

10. (original) Apparatus as claimed in claim 8, further comprising a router connected to the intrusion detection sensor for rerouting, in response to generation of the alert signal, any data traffic originating at the address assigned to the data

processing system originating the data indicative of the attack to a disinfection address on the network.

11. (original) Apparatus as claimed in claim 8, wherein the intrusion detection sensor, on generation of the alert signal, sends an alert message to the disinfection address.

12. (original) Apparatus as claimed in claim 11, wherein the alert message comprises data indicative of the attack detected.

13. (original) Apparatus as claimed in claim 12, further comprising a disinfection server assigned to the disinfection address, the disinfection server sending, on receipt of the alert message, a warning message to the address assigned to the data processing system originating the data indicative of the attack.

14. (original) Apparatus as claimed in claim 13, wherein the warning message comprises program code for eliminating the attack when executed by the data processing system originating the data indicative of the attack.

15. (currently amended) A data communications network comprising: a plurality of addresses for assignment to data processing systems in the network; and, apparatus for detecting attacks on the network as claimed in claim 8 ~~any of claims 8 to 14~~.

16. (currently amended) A computer program element comprising computer program code means which, when loaded in a processor of a data processing system, configures the processor to perform a method for detecting attacks on a data communications network as claimed in claim 1 ~~any of claims 1 to 7~~.

17. (original) A method as claimed in claim 1, further comprising supporting an entity in the handling of the detected attack by one of providing instructions for use of, assistance in executing, and execution of disinfection program code.

18. (original) A method as claimed in claim 1, further comprising providing a report to said entity containing information related to one of alert, disinfection, rerouting, logging, discarding of data traffic in the context of a detected attack.

19. (original) A method as claimed in claim 1, further comprising billing said entity for the execution of at least one of the steps contained in claim 1 ~~claims 1 to 7~~, the charge being billed preferably being determined in dependence of one of the size of the network, the number of unassigned addresses monitored, the number of assigned addresses monitored, the volume of data traffic inspected, the number of attacks identified, the number of alerts generated, the signature of the identified attack, the volume of rerouted data traffic, the degree of network security achieved, the turnover of said entity.

20. (original) A method as claimed in claim 1, further comprising providing said method for several entities and using technical data derived from the attack-handling for one of said entities for the attack-handling for another of said entities.

21. (currently amended) A method for deploying an intrusion detection application for an entity, comprising:
connecting an intrusion detection sensor to a network used by said entity for identifying data traffic on the network originating at any assigned address and addressed to any unassigned address, said unassigned address is an address which is free and not assigned to user systems, and for inspecting any

data traffic so identified for data indicative of an attack and for, on detection of data indicative of an attack, generating an alert signal,

- connecting a router to said network for rerouting, in response to generation of the alert signal, any data traffic originating at the address assigned to the data processing system originating the data indicative of the attack to a disinfection address on the network.

22. (original) A method according to claim 21, further comprising

- connecting a disinfection server assigned to the disinfection address, to the network, the disinfection server being adapted for sending, on receipt of the alert message, a warning message to the address assigned to the data processing system originating the data indicative of the attack.

23. (new) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing detection of attacks on a data communications network having a plurality of addresses for assignment to data processing systems in the network, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1.

24. (new) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing deployment of an intrusion detection application for an entity, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 21.